Veranda

# INCIDENT MANAGEMENT POLICY

## CHANGE HISTORY

| Date | Version | Created by | Approved By | Description of change |
|---|---|---|---|---|
| 08/10/2024 | 1.0 | Bharath S | Ashwin Khosla | Basic document outline and submitted for review |

## Purpose

The purpose of the Incident Management Policy is to outline the procedures in place at Veranda Learning to monitor, alert, respond and mitigate security incidents.

## Scope

Incident management policy applies to

- All Employees of Veranda Learning
- All Contractors of Veranda Learning
- All information management systems in Veranda Learning

## Background

Security incidents happen, and the best thing an organization can do for its customers is to be best prepared for them when it happens. Incident Management policy outlines the procedures for managing security incidents at Veranda Learning. It outlines the procedures in place to ensure that

- Proper controls are in place to monitor and alert when security incidents happen.
- The right team is identified, trained, and available to investigate and resolve the security incidents.
- Proper communication channels and SLAs are in place with the customer to inform the customer of the incident.
- Proper learnings and corrective actions are captured and iteratively applied to improve incident response procedures.

## Policy

Veranda Learning incident response policy is based on NIST Special Publication 800-61. Revision 2. Refer to this NIST publication to create a detailed Incident Response Plan for Veranda Learning

This Incident Response Policy establishes objectives for creating and maintaining Veranda Learning's Incident Response Plan. Veranda Learning's incident response plan shall address the following areas and steps for effective incident identification, resolution, and remediation.

- Be prepared to handle an incident
- Identify and report an incident
- Incident assignment
- Incident analysis & resolution
- Resolution communication
- Review, analysis, and learnings

**Be prepared to handle an incident.**

Veranda Learning takes the following preparatory steps to handle security incidents

- Implements relevant security controls such as encryption, strong passwords, MFA, awareness training along with other tools and processes to prevent security incidents
- Easily accessible contact information and on-call information
- Easy issue-reporting mechanism
- Monitoring tools on Veranda Learning's network, servers, and other devices to preemptively detect incidents
- Analysis tools for network traffic and file systems are in place to analyze events as they happen or post-event

- Documentation and training resources are available to the incident response team.

### Identify and report an incident.

Incidents are events at Veranda Learning or at its suppliers/vendors that potentially or actually compromise Veranda Learning's information, which is known or reasonably believed to have resulted in:

- Unauthorized access or acquisition of Customer, Employee, Partner, Supplier, or proprietary data
- Unauthorized access to information systems, whether in-house or in the Cloud
- Unauthorized modification of the Company's public-facing websites or services or a substantially distributed denial of service (DDoS)
- Loss or theft of a laptop, computer, or portable device (e.g., a Smartphone, flash drive, tablet, CD/DVD, or other mobile media device) containing the Company's personal or business data, and the device is not encrypted.
- Loss or theft of paper records or files containing Company personnel or business data.

Notification of a breach or 'hack' of a Veranda Learning's third-party vendor, partner, or supplier may also be considered a security incident where the above criteria are met.

### Reporting incidents

- Incidents can be detected and automatically reported by monitoring tools or manually reported by personnel if they observe a breach of any security policy, acceptable use policy, or code of conduct policy.
- A ticket management system is in place to assist in reporting and tracking all incidents. All security incidents are reported within the ticketing system.
- All security incidents are classified as follows with appropriate resolution SLAs after which the security incidents are escalated to the office of the CISO.
  - Critical: Catastrophic issue which can lead to severe damage to Company's reputation (Resolve: 4 hours)
  - Major: Issue which affects the operation of one information system and can cause damage if not resolved quickly (Resolve: 8 hours)
  - Minor: Small issue most related to noncompliance or deviation from best practices that do not cause significant damage (Resolve: 48 hours)
  - Cosmetic: Documentation or a policy issue that can be resolved via documentation (Resolve: 7 days)
- All evidence, such as logs, files, and traces, must be attached to the incident ticket evidence.
- Evidence may also be classified based on the impact of the classified data.
  - Privacy beach - involving PII
  - Proprietary breach - involving critical infrastructure
  - Integrity loss: Loss of data and information

### Assign to Incident Response Team

- An incident response team that is appropriately trained in handling incidents on impacted information systems is assigned to the Incident to
  - Investigate
  - Resolve
  - Perform root cause analysis
  - Make recommendations for future mitigation.
- The team is available 24 / 7 to respond to any incident.
- Other management team members from HR, Customer Success, and Legal also get involved based on the issue priority.

- The Incident response team documents the resolution and captures all evidence, such as logs, to present to the law enforcement authorities if needed.
- External parties such as law enforcement and other government bodies may be involved to assist in the Incident.

**Incident analysis & resolution**

The incident response team analyzes the Incident based on the type of threat, impact on the data, potential damage or theft of resources, and impact on service availability (e.g., network connectivity, services provided to external parties), among other factors.

Incident response teams create a containment strategy for the Incident and provide the time and resources needed to implement the strategy (e.g., an emergency workaround in four hours, a temporary workaround in two weeks, and a permanent solution in one month).

Example containment strategies created by Incident Response Team

- Redirect attackers to a sandbox (a form of containment) so that they can monitor the attacker's activity, usually to gather additional evidence
- Disconnecting and isolating a malicious host from the network
- Eradicating malware etc
- Identifying attacking hosts
- Involving governing and law enforcement bodies

**Resolution communication**

- The incident response team maintains a communication plan that includes email templates, distribution lists of customers, vendors, and other parties, contacts of authorities and management, and timeliness of communication.
- Senior management of Veranda Learning is notified before a customer is notified.
- All affected customers are informed within 24 hours of incidents.
- The communication contains a description, the status of the resolution, root cause, mitigation, and next steps, if any.
- If required, law enforcement is notified of the Incident.
- Other government bodies and media are involved and communicated as required.

**Review, analysis, and learnings**

After the Incident is contained or resolved, Veranda Learning performs a post-mortem of the Incident to prevent the Incident from repeating. The following information is gathered and recorded for learning and training purposes.

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the Incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for to detect similar incidents in the future?

After every significant Incident, the incident response team evaluates the following items against applicable regulations, policies, and generally accepted practices:

- Tools and resources

- Team model and structure
- Incident handler training and education
- Incident documentation and reports

**Evidence retention**

All evidence is retained as per the data retention policy.

## Mapping with Industry Standards

This policy addresses the following risks related to Incident Management and Information Security standards, frameworks:

| Risk | Mapping with ISO 27001:2022 |
|---|---|
| Denial of Service | 6.8 Information security event reporting<br>5.26 Response to information security incidents<br>C 8.1 Operational planning and control |
| Unauthorized Use of Information assets | 5.24 Information security incident management planning and preparation<br>5.28 Collection of evidence<br>5.26 Response to information security incidents<br>5.27 Learning from information security incidents<br>5.5 Contact with authorities |
| Unauthorized access | 5.28 Collection of evidence<br>5.26 Response to information security incidents<br>5.5 Contact with authorities |
| Information Leakage | 5.25 Assessment and decision on information security events<br>5.28 Collection of evidence<br>5.26 Response to information security incidents<br>C 8.1 Operational planning and control |
| Theft | 5.28 Collection of evidence<br>5.26 Response to information security incidents<br>C 8.1 Operational planning and control |
| Physical Loss or damage | 5.28 Collection of evidence<br>5.26 Response to information security incidents<br>C 8.1 Operational planning and control |

## Enforcement

Incident management policy is enforced by the information security team. All exceptions to the policy should be brought to the attention of the information security team along with the executive management of the company.

## Non- Compliance

Violations of the policy may subject employees to disciplinary action, including removal of privilege to the systems, up to and including termination of employment. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

- Disciplinary action according to applicable Veranda learning policies.

- Termination of employment.
- Legal action according to applicable laws and contractual agreements.

## Validity and Document Management

The owner of this document is the management, who must check and, if necessary, update the document at least once every 12 months.